REMARKS

Claims 29 through 48 were presented for examination and were pending in this application. In a Final Office action dated August 11, 2005, ("Office action") claims 29 through 48 were rejected. Applicants thank Examiner for examination of the claims pending in this application and address Examiner's comments below.

Applicants herein amend claims 29-41 and 43-48. No claims are deleted or added. Applicants respectfully submit that these changes merely correct ministerial errors such as improper antecedent basis and spellings. They are believed not to introduce new matter and their entry is respectfully requested. In making this amendment, Applicants have not and do not narrow the scope of the protection to which Applicants consider the claimed invention to be entitled and do not concede that the subject matter of such claims was in fact disclosed or taught by the cited references. Rather, Applicants reserve the right to pursue additional protection at a later point in time.

Based on the following Remarks, Applicants respectfully request that Examiner reconsider all outstanding rejections, and withdraw them.

Reply to Examiner's Response to Arguments

On page 2 of the Office action, Examiner misunderstands the feature of the detector device not introducing a point of failure in the network. Examiner alleges that operational failure of the detector device introduces a point of failure because various claim features cannot occur if the detector device fails. In claims 29, 36, and 43, operational failure is recited as a non-functioning operation. Thus, even with a non-functioning operation, the operational failure of the detector device does not introduce a point of failure *in the network.* In fact, the network remains functional because signals will continue to pass through the network unimpeded by the non-functioning operations in the detector device. Specification, page 4, lines 11-14; page 10, lines 21- page 11, line 5; page 11, lines 11-17; Amendment G dated March 31, 2005, page 11; Amendment F dated August 3, 2004, page 10; Amendment E dated February 19, 2004, page 9. Therefore, non-functioning operations in the detector device do not introduce a point of failure *in the network*, allowing transactions between devices to continue unimpeded.

On page 3 of the Office action, Examiner states: "Examiner interprets these claims wherein the request signals simply pass uninterrupted between a first device and a second device through a failed detector device on an intermediary device within the network and the above steps recited in the claims do not occur." Examiner's claim interpretation is improper because it fails to consider every limitation in the claims.

M.P.E.P. § 2106(II)(C) clearly instructs examiners to "begin claim analysis by identifying and evaluating each claim limitation," and "when evaluating the scope of a claim, <u>every</u> limitation in the claim must be considered" (emphasis in original). Unfortunately, Examiner's claim interpretation fails to consider *most* of the claim limitations recited in independent claims 29, 36 and 43. These claims recite several operational aspects of a detector device that has not failed. Following are just a few examples of claim limitations *completely ignored* by Examiner's approach: "generating a response to the request signal to alter communications between the first device and the second device in response to the comparison providing a first result and not altering communications between the first device and the second device in response to the comparison providing a second result" as recited in claim 29, "identifying a credit balance for the user identification" as recited in claim 36, and "determining whether a user identified by the user identification parameter in a request signal of the plurality of request signals and associated with the first device is permitted access to data associated with the second device" as recited in claim 43. Moreover, the step of allowing signals to pass uninterrupted occurs in response to a non-functioning operation within the detector device. Thus, Applicants respectfully request Examiner to determine the scope of claims by considering every claim limitation and to withdraw the improper claim interpretation approach used on pages 3-4 of the Office action.

Response to Rejections Under 35 U.S.C. § 102

In the Office action, Examiner rejects claims 29-48 under 35 U.S.C. § 102(b) as allegedly being anticipated by "Teach Yourself TCP/IP in 14 days" ("TCP/IP"). Examiner also rejects claims 29-48 under 35 U.S.C. § 102(a) as allegedly being anticipated by Official Notice. Further, Examiner rejects claims 29-48 under 35 U.S.C. § 102(a) as allegedly being anticipated by Applicants' allegedly admitted prior art. All of these rejections are respectfully traversed.

Claim 29 is directed to a method for use in a detector device for controlling access to information on a network including a plurality of interconnected devices. The detector device is coupled to the network between a first device and a second device. As amended, the method recites:

> monitoring, independent of the first device and the second device, a plurality of request signals between the first device and the second device in the network, at least one request signal including a user identification parameter;

determining whether a user identified by the user identification parameter in the at least one request signal is permitted access to data being requested;

comparing a predetermined parameter associated with the user with a predetermined parameter associated with the data to determine permission to access the data; and

generating a response to the request signal to alter communications between the first device and the second device in response to the comparison providing a first result and not altering communications between the first device and the second device in response to the comparison providing a second result, the detector device allowing the plurality of request signals to pass uninterrupted between the first device and the second device regardless of the first result or the second result in response to an operational failure of the detector device, the operational failure comprising a non-functioning operation.

Claim 36 is directed to a network-based billing method for use in a detector device for providing access to resources on a network. The detector device is coupled to the network such that it does not introduce a point of failure. As amended, the method recites:

monitoring, independent from the resources, a data signal from a device on the network, the data signal including a request for a resource;

identifying a value for accessing the resource;

associating a user identification with the data signal;

determining whether a user identified by the user identification is permitted access to the resource;

identifying a credit balance for the user identification;

comparing the credit balance with the value to determine whether access to the resource is permissible;

in response to the comparison, determining a response to the request for the resource; and

in response to an operational failure within the detector device, allowing data signals to pass uninterrupted between the resources on the network, the operational failure comprising a non-functioning operation.

Claim 43 is directed to a detector device capable of controlling access to information on a network including a plurality of interconnected devices. As amended, the device comprises:

a processing unit within the detector device coupled to the network between a first device and a second device, the detector device independent of the first device

and the second device, the processing unit configured to execute instructions, the instructions including:
monitoring a plurality of request signals between the first device and the second device in the network, at least one request signal including a user identification parameter;
determining whether a user identified by the user identification parameter in a request signal of the plurality of request signals and associated with the first device is permitted access to data associated with the second device;
comparing a predetermined parameter associated with the user with a predetermined parameter associated with the data to determine permission to access the data;
providing a response to the request signal of the plurality of request signals in response to the comparison; and
allowing the plurality of request signals to pass uninterrupted between the first device and the second device in response to an operational failure within the detector device, the operational failure comprising a non-functioning operation.

The claimed invention provides a detector device capable of controlling access to information or resources on a network by monitoring signals on the network. Upon detecting a signal on the network, the detector device determines whether a user is permitted to access a resource or data associated with a signal. The detector device also compares a parameter associated with the user, e.g. a credit balance for the user, with a parameter associated with the data/resource, e.g. a value for accessing the resource, to determine permission to access the data/resource. Based on the comparison, the detector device determines a response to the signal, e.g. altering communications between network devices. Accordingly, when the detector device is operational it is capable of controlling access to network resources and data. Moreover, signals on the network are able to pass uninterrupted in response to an operational failure within the detector device, the operational failure comprising a non-functioning operation. Hence, the claimed invention provides a robust monitoring and processing system without introducing a point of failure within the network.

Neither TCP/IP nor Applicants' allegedly admitted prior art, either alone or in combination, disclose, teach or suggest the claimed invention. Nor does Examiner's Official Notice of a conventional gateway, router, or proxy disclose, teach or suggest the claimed invention.

For a rejection under 35 U.S.C. 102(a) or 102(b), each element in a claim must be disclosed by a reference. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Citing Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); M.P.E.P. § 2131. Examiner's rejection is improper because the cited references fail to disclose at least the following claim limitations.

i. Allowing signals to pass uninterrupted in response to an operational failure of the detector device.

Claim 29, as amended, recites: "the detector device allowing the plurality of request signals to pass uninterrupted between the first device and the second device regardless of the first result or the second result in response to an operational failure of the detector device, the operational failure comprising a non-functioning operation." Claim 36, as amended, recites: "in response to an operational failure within the detector device, allowing data signals to pass uninterrupted between the resources on the network, the operational failure comprising a non-functioning operation." Claim 43, as amended, recites: "allowing the plurality of request signals to pass uninterrupted between the first device and the second device in response to an operational failure within the detector device, the operational failure comprising a non-functioning operation." Neither TCP/IP, nor Applicants' allegedly admitted prior art, nor a conventional gateway, router, or proxy, disclose these features of independent claims 29, 36 and 43.

According to one embodiment of the claimed invention shown in figure 3 of the present application, the detector device merely observes or samples signals passing through a connector node 312 without impeding the signals. Specification, page 11, lines 11-17. Hence, even if the detector device experiences a non-functioning operation, the signals will continue to pass through the connector node 312. Specification, page 4, lines 11-14; page 10, lines 21-27; Amendment G dated March 31, 2005, page 11; Amendment F dated August 3, 2004, page 10; Amendment E dated February 19, 2004, page 9. Therefore, the detector device does not introduce a point of failure in the network.

The portion of TCP/IP cited by Examiner on page 5 of the Office action merely identifies a conventional gateway whose "sole task is to receive a Protocol Data Unit (PDU) from either the internetwork or the local network and either route it on to the next gateway or pass it into the local network for routing to the proper user." TCP/IP, page 45. When such a gateway experiences operational failure, it is *incapable* of continuing to route PDUs because each PDU must pass through the gateway. The PDUs will no-longer pass through a gateway if the gateway fails. Therefore, TCP/IP fails to disclose or suggest a detector device that allows signals to pass uninterrupted in response to an operational failure.

On pages 8-9 of the Office action, Examiner takes Official Notice of a gateway or router or proxy as devices that allow signals to pass through. Similarly, on pages 9-10 of the Office action, Examiner alleges that Applicants' admitted prior art discloses a proxy server that allows packets to pass through. As explained above, data is *unable* to pass uninterrupted through a gateway or router that experiences operational failure. Moreover, as explained in the specification, proxy server 108 impedes the flow of data if it is not functioning properly. Figure 1A; Specification, page 9, lines 8-19. Specifically, "[i]f the proxy server 108 is not functioning properly, then the overall flow of data would be adversely affected. If the proxy server 108 fails, then the data flow would cease altogether." Specification, page 9, lines 13-15. Neither a proxy server nor a gateway or router would allow signals to pass uninterrupted in response to an operational failure. Therefore, a gateway, router or a proxy server, either alone or in combination, fail to disclose or suggest a detector device that allows signals to pass uninterrupted in response to an operational failure.

For at least the above reasons, Examiner is respectfully requested to withdraw the "Official Notice" rejection as it improperly isolates elements out of the context of the claims as a whole. Further, if Examiner wishes to maintain this rejection, Examiner is requested to provide actual references that are relevant to the examination of the claims rather than rely on mere "Official Notice" as a basis of support for the rejection.

ii. Comparing a parameter associated with the user with a parameter associated with the data/resource to determine permission to access the data/resource.

To provide another example of claim features neither disclosed nor suggested by the cited references, claim 29, as amended, recites: "comparing a predetermined parameter associated with the user with a predetermined parameter associated with the data to determine permission to access the data." Claim 36, as amended, recites: "comparing the credit balance with the value to determine whether access to the resource is permissible." Claim 43, as amended, recites: "comparing a predetermined parameter associated with the user with a predetermined parameter associated with the data to determine permission to access the data." Neither TCP/IP, nor Applicants' allegedly admitted prior art, nor a conventional gateway, router, or proxy, disclose or suggest these features of independent claims 29, 36 and 43.

According to one embodiment of the claimed invention, the detector device compares a parameter associated with the user with a parameter associated with the data/resource to determine permission to access the data/resource. For example, the detector device allows a user to access a news article if the user's credit balance meets the required value, e.g. cost, of accessing the resource.

The portion of TCP/IP cited by Examiner on page 5 of the Office action merely identifies a conventional gateway whose "sole task is to receive a Protocol Data Unit (PDU) from either the internetwork or the local network and either route it on to the next gateway or pass it into the local network for routing to the proper user." TCP/IP, page 45. However, the cited portions of TCP/IP fail to disclose or suggest controlling access to data or a resource by comparing a parameter associated with the user to a parameter associated with the data/resource. Moreover, Examiner's Official Notice rejection on pages 8-9 of the Office action merely identifies a gateway, router or proxy without providing any disclosure, hint or suggestion of controlling access to data or a resource by comparing a parameter associated with the user to a parameter associated with the data/resource. Once again, Examiner is requested to provide actual references that are relevant to the context of the claims rather that rely on feeble "Official Notice" as a basis of support to maintain this rejection.

Similarly, Examiner's rejection on pages 9-10 of the Office action merely refers to a proxy server discussed on page 9, lines 9-19 of the specification. However, this portion of the specification provides no disclosure or suggestion of a proxy server controlling access to data or a resource by comparing a parameter associated with the user to a parameter associated with the data/resource. Therefore, TCP/IP as well as a conventional gateway, router, or proxy fails to disclose or suggest a detector device capable of comparing a parameter associated with the user with a parameter associated with the data/resource to determine permission to access the data/resource.

In sum, it is abundantly clear that independent claims 29, 36 and 43 are allowable because each cited reference fails to disclose or suggest the above limitations, either alone or in combination for at least the reasons set forth above. Further, dependent claims 30-35, 37-42 and 44-48 depend from claims 29, 36 and 43, and are allowable at least for the same reasons as independent claims 29, 36 and 43.

Therefore, Applicants respectfully request reconsideration and removal of all rejections to claims 29 through 48. Applicants also request allowance of these claims at this time.

Conclusion

In conclusion, Applicants respectfully submit that claims 29 through 48, as presented herein, are patentably distinguishable over the cited references (including references cited, but not applied). Therefore, Applicants request reconsideration of the basis for the rejections to these claims and request allowance of them.

In addition, Applicants respectfully invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
Stanislav Khirman, Mark Ronald Stone, Oren Arial and Ori Cohen

Date: November 14, 2005 By: Raj P Patel

Rajiv P. Patel, Attorney of Record
Registration No. 39,327
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7607
Fax: (650) 938-5200